JOURNAL OF NUMBER THEORY **65**, 321–324 (1997)
ARTICLE NO. NT972129

On the Binary Digits of a Power

Bernt Lindström

Department of Mathematics, Royal Institute of Technology, S-100 44 Stockholm, Sweden

Communicated by V. T. Sós

Received September 2, 1996

IN MEMORY OF PAUL ERDŐS

same result with m^h replaced by any polynomial $a_0 m^h + a_1 m^{h-1} + \cdots + a_h$ with integer coefficients and $a_0 > 0$. © 1997 Academic Press

1. INTRODUCTION

Let $B(m)$ denote the number of ones in the binary expansion of the integer $m \geqslant 0$. For positive integers h and p and $m < 2^p$ we have then $B(m^h)/p < h$. Numerical calculations by Bengt Rosén in Linköping gave $\sup B(m^2) = 34$ for $m < 2^{20}$. This supremum was first attained by $m = 980853$ giving $B(m^2)/\log_2 m \approx \#1.708$. It seemed hard to beat this record. For example, $\sup B(m^2)$ for $m < 2^{26}$, first attained by $m = 57804981$, gives a smaller value. Nevertheless we can prove:

THEOREM. *$\limsup_{m \to \infty} B(m^h)/\log_2 m = h$ for $h \geqslant 2$. The same result holds with m^h replaced by any $a_0 m^h + a_1 m^{h-1} + \cdots + a_h$ with integer coefficients and $a_0 \geqslant 1$.*

We may mention that the problem of bounding $B(m^h)/B(m)$ has been studied by Stolarsky [1], but this is a different problem.

2. PROOF

We shall use numbers m with *noninterfering* terms. Consider the simple examples $a2^p \pm b$ with $a, b \geqslant 1$ and $b < 2^p$. Then terms are nontinterfering

0022-314X/97 $25.00

and $B(a2^p+b)=B(a)+B(b)$, $B(a2^p-b)=B(a-1)+p-B(b-1)$. With $b\geqslant 2^p$ the terms will interfere and we cannot use these formulas.

We start the proof by choosing an integer $k\geqslant 2$ and define the integer $q=\lfloor \log_2 k\rfloor+2h+1$. Then we have

$$k<2^{q-2n-1} \qquad (1\leqslant n<h). \tag{1}$$

Define for $p>q$ the integers m_p by

$$m_p=2^{pk}-\sum_{i=1}^{k-1} 2^{pi-q}+1 \tag{2}$$

and a polynomial $m(X)$ by

$$m(X)=2^q X^k-\sum_{i=1}^{k-1} X^i+2^q \tag{3}$$

Then we have

$$m(2^p)=m_p 2^q. \tag{4}$$

Next we define the integers $D_{j,i}^{(n)}$ $(1\leqslant i\leqslant k;\ 1\leqslant j\leqslant n)$ for $n\geqslant 1$ by

$$(m(X))^n=\sum_{j=1}^{n}\left(D_{j,k}^{(n)} X^{jk}-\sum_{i=1}^{k-1} D_{j,i}^{(n)} X^{(j-1)k+i}\right)+2^{nq} \tag{5}$$

and integers $E_{j,i}^{(n)}$ $(1\leqslant i\leqslant 2k-1;\ 1\leqslant j\leqslant n)$ by

$$\left(\sum_{i=1}^{k-1} X^i\right)\left(\sum_{i=1}^{k-1} D_{j,i}^{(n)} X^i\right)=\sum_{i=1}^{2k-1} E_{j,i}^{(n)} X^i. \tag{6}$$

We define for convenience when $n\geqslant 1$

$$\begin{aligned} &D_{0,i}^{(n)}=D_{n+1,i}^{(n)}=0 \qquad (1\leqslant i<k), \quad D_{0,k}^{(n)}=2^{nq}, \quad D_{n+1,k}^{(n)}=0,\\ &E_{0,i}^{(n)}=E_{n+1,i}^{(n)}=0 \qquad (1\leqslant i<2k). \end{aligned} \tag{7}$$

If we multiply (5) by $m(X)$ and use (3), (5), and (7), we find $(n\geqslant 1)$

$$\begin{aligned} D_{j,i}^{(n+1)}&=2^q D_{j-1,i}^{(n)}+2^q D_{j,i}^{(n)}+D_{j-1,k}^{(n)}-E_{j,i}^{(n)}-E_{j-1,k+i}^{(n)} \qquad (1\leqslant i<k)\\ D_{j,k}^{(n+1)}&=2^q D_{j-1,k}^{(n)}+2^q D_{j,k}^{(n)}+E_{j,k}^{(n)} \qquad (1\leqslant j\leqslant n+1). \end{aligned} \tag{8}$$

For $n=1$ we have by (3) and (5)

$$D_{1,i}^{(1)}=1 \qquad (1\leqslant i<k), \quad D_{1,k}^{(1)}=D_{0,k}^{(1)}=2^q. \tag{9}$$

By induction over $1\leqslant n\leqslant h$ we find using (8) and (9)

$$\begin{aligned} 0<D_{j,i}^{(n)}&<2^{(n-1)q+2n} && (1\leqslant i<k),\\ 2^{nq}\leqslant D_{j,k}^{(n)}&<2^{nq+2n} && (1\leqslant j\leqslant n),\\ 0\leqslant E_{j,i}^{(n)}&<2^{nq-1} && (1\leqslant i<2k;\ 1\leqslant j\leqslant n). \end{aligned} \tag{10}$$

The last inequality follows by (1), (6), and (10). The inequality $D_{j,i}^{(n+1)}>0$ follows since $E_{j,i}^{(n)}+E_{j-1,k+i}^{(n)}<2^{nq}\leqslant D_{j-1,k}^{(n)}$.

The coefficients of $(m(X))^h$ are bounded by 2^{hq+2h}. If we choose $p\geqslant hq+2h$ then the terms of $(m_p 2^q)^h=m(2^p)^h$ (by (4)) will be noninterfering and we find easily the bounds

$$\begin{aligned} hp(k-1)-h^2(k-1)(q+2)&<B(m_p^h)\\ &<hp(k-1)+h^2(q+2)+1, \end{aligned} \tag{11}$$

which implies that $\lim_{p\to\infty} B(m_p^h)/\log_2 m_p=h(1-k^{-1})$. Then let $k\to\infty$ and the theorem follows for powers of m_p.

We consider now the general case with a polynomial in place of m^h. First we assume that all coefficients are nonnegative integers and let

$$\begin{aligned} F(X)&=a_0 m(X)^h+a_1 2^q m(X)^{h-1}+\cdots+2^{hq}a_h,\\ f(X)&=a_0 X^h+a_1 X^{h-1}+\cdots+a_h. \end{aligned} \tag{12}$$

Then we have

$$F(2^p)=2^{hq}f(m_p). \tag{13}$$

By (5) and (12) there are integers $F_{j,i}$ $(1\leqslant i\leqslant k;\ 1\leqslant j\leqslant h)$ such that

$$F(X)=\sum_{j=1}^{h}\left(F_{j,k}X^{jk}-\sum_{i=1}^{k-1}F_{j,i}X^{(j-1)k+i}\right)+2^{hq}f(1). \tag{14}$$

And by (10) we find the bounds

$$\begin{aligned} 0<F_{j,i}&<2^{(h-1)q}f(4) && (1\leqslant i<k;\ 1\leqslant j\leqslant h),\\ 2^{hq}\leqslant F_{j,k}&<2^{hq}f(4) && (1\leqslant j\leqslant h). \end{aligned} \tag{15}$$

If we choose $p \geqslant hq + \log_2 f(4)$ then the terms of $F(2^p)$ will be noninterfering and we find bounds for $B(F(2^p)) = B(f(m_p)$ similar to (11) giving $\lim_{p\to\infty} B(f(m_p))/\log_2 m_p = h(1-k^{-1})$.

If there are negative integers among the coefficients $a_1, a_2, ..., a_h$ then we may find an integer A such that the polynomial $f(X+A)$ has nonnegative coefficients. Thus we need only replace m_p by $m_p + A$ in order to get the same limit as before. Then let $k \to \infty$ and the theorem follows.

REFERENCE

1. K. B. Stolarsky, The binary digits of a power, *Proc. Amer. Math. Soc.* **71** (1978), 1–5.